Abstract

The essence of the invention is in that when making a digital blind RSA-signature a new technique for blinding an initial data by a RSA-encryption and corresponding technique for unblinding the signed blinded data are employed, which gives the possibility to use an unlimited number of kinds of the signature in electronic systems of the mass scale service. The untraceability is ensured by a corresponding choice of the randomized exponent R, RSA-key used in RSA-encryption the initial data, and by the public module N properties verified in an arbitrary time moment. In so doing, $N=P\cdot Q$, where P and Q are secret prime factors, and R is multiple to $N-1$. In other variants of the invention the diversity of kinds of the signature is set by limitings on multiplicities of public exponents, said limitings being chosen prior to blinding the initial data. The apparatus to realize the method for making a digital blind RSA-signature comprises a blinding unit based on a modular exponentiator, and a corresponding unblinding unit.